
Vulnerability Assessment & Penetration Testing
Report of
SmartCare Remote Management Web Application – Failed Cases

Dec 2022

About L&T Technology Services:

L&T Technology Services Limited (LTTS) is a global leader in Engineering and R&D (ER&D) services. With 399 patents filed for 51 of the Global Top 100 ER&D spenders. Our innovations speak for itself – World's 1st Autonomous Welding Robot, Solar 'Connectivity' Drone, and the Smartest Campus in the World, to name a few. LTTS expertise in engineering design, product development, smart manufacturing, and digitalization touches every area of our lives. With 49 Innovation and R&D design centres globally, we specialize in disruptive technology spaces such as 5G, Artificial Intelligence, Collaborative Robots, Digital Factory, and Autonomous Transport. **LTTS is a publicly listed subsidiary of Larsen & Toubro Limited, the \$18 billion Indian conglomerate operating in over 30 countries.**

Document History:

Var. Rel. No.	Release Date	Prepared By. Prepared. Dt.	Reviewed By Reviewed Dt.	Approved By Approval Dt.	Remark/Revision Details
1.0	Dec 2022	Sanidya Sharan Sai Praneetha Bhaskaruni	Sunil M.C	Atanu Niyogi	
		14 th Dec 2022			

Table of Contents

1. Overview of the project	5
3. Abbreviation	23

1. Overview of the project

L&T Technology Services (LTTS) has conducted Security Assessment for the SmartCare Remote Management web application. The purpose of the assessment is to evaluate the security posture of the web application against common vulnerabilities.

Objective of the security assessment:

As a part of this engagement a holistic approach was taken to conduct the Vulnerability Assessment and Penetration Testing on the SmartCare Remote Management web application. During the engagement High, Medium, and Low severity issues were identified with respect to the SmartCare Remote Management web application.

Approach

The following approach was taken to make sure the target was assessed against known vulnerabilities from all possible security perspectives:

- Manual Vulnerability Assessment and Penetration Testing of using OWASP Top 10 for web applications.

Some of the tools which were used are listed below:

Target Product	SmartCare Remote Management web application
Browser	Chrome, Firefox
Tools	Burp Suite, Nmap, Whatweb, SQLMap, DirBuster, Curl, Httpprint

Key Security Policies

OWASP top 10 listed vulnerabilities were used as a reference Standard. The following key security aspects were checked:

Sr No	OWASP Top 10
1	Broken Access Control
2	Cryptographic Failures
3	Injection
4	Insecure Design
5	Security Misconfiguration
6	Vulnerable and Outdated Components
7	Identification and Authentication Failures
8	Software and Data Integrity Failures
9	Security Logging and Monitoring Failures
10	Server-Side Request Forgery

The Failed cases where attack vectors were carried out, but the web application did not have the vulnerability is listed below

1. Fingerprint Web Server:

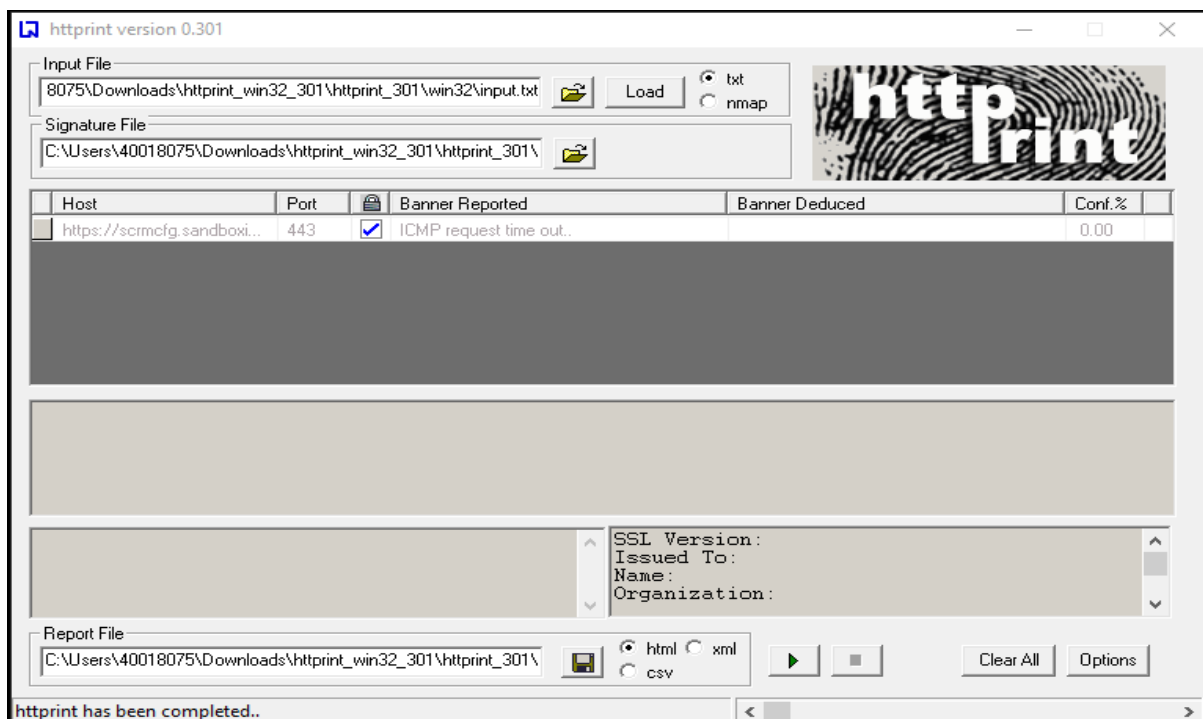
Description:

Discovering the type of web server that an application runs on can enable security testers to determine if the application is vulnerable to attack. In particular, servers running older versions of software without up-to-date security patches can be susceptible to known version-specific exploits.

Expected Output:

It was expected to identify the type and version of web server.

PoC (Proof of Concept):



2. Webserver Metafiles for Information Leakage:

Description:

Test various metadata files for information leakage of the web application's path(s), or functionality. Furthermore, the list of directories that are to be avoided by Spiders, Robots, or Crawlers can also be created as a dependency for map execution paths through application.

Expected Output:

We analysed the robots.txt" functions and web server metafiles.

PoC (Proof of Concept):

```

myts100594@myts100594-Latitude-3400: $ curl https://scrmcfg.sandboxiot.hillrom.com/apps/remotemanagement/index.html -v
* Trying 20.81.62.223:443...
* Connected to scrmcfg.sandboxiot.hillrom.com (20.81.62.223) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* CAfile: /etc/ssl/certs/ca-certificates.crt
* CApath: /etc/ssl/certs
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: CN=*.sandboxiot.hillrom.com
* start date: Jan 14 13:27:03 2022 GMT
* expire date: Feb 15 13:27:03 2023 GMT
* subjectAltName: host "scrmcfg.sandboxiot.hillrom.com" matched cert's "*.sandboxiot.hillrom.com"
* issuer: C=US; ST=Arizona; L=Scottsdale; O=GoDaddy.com, Inc.; OU=http://certs.godaddy.com/repository; CN=Go Daddy Secure Certificate Author
* ty - G2
* SSL certificate verify ok.
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* GET /apps/remotemanagement/index.html HTTP/1.1
* Host: scrmcfg.sandboxiot.hillrom.com
* User-Agent: curl/7.81.0

```

3. Enumerate Applications on Webserver:

Description:

Testing for web application vulnerabilities is to find out which particular applications are hosted on a web server. We know that vulnerabilities and known attack strategies that can be exploited in order to gain remote control or to exploit data.

Expected Output:

We tried to enumerate the applications within the scope that exist on a web server.

PoC (Proof of Concept):

```

Target: scrmcfg.sandboxiot.hillrom.com Profile: Intense scan
Command: nmap -T4 -A -v scrmcfg.sandboxiot.hillrom.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
scrmcfg.sandboxio

nmap -T4 -A -v scrmcfg.sandboxiot.hillrom.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 16:13 India Standard Time
NSOCK ERROR [0.2660s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating Ping Scan at 16:13
Scanning scrmcfg.sandboxiot.hillrom.com (20.81.62.223) [4 ports]
Completed Ping Scan at 16:13, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:13
Completed Parallel DNS resolution of 1 host. at 16:13, 0.20s elapsed
Initiating SYN Stealth Scan at 16:13
Scanning scrmcfg.sandboxiot.hillrom.com (20.81.62.223) [1000 ports]
Discovered open port 80/tcp on 20.81.62.223
Completed SYN Stealth Scan at 16:13, 15.31s elapsed (1000 total ports)
Initiating Service scan at 16:13
Scanning 2 services on scrmcfg.sandboxiot.hillrom.com (20.81.62.223)
Service scan Timing: About 50.00% done; ETC: 16:15 (0:01:01 remaining)
Completed Service scan at 16:14, 61.86s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against scrmcfg.sandboxiot.hillrom.com (20.81.62.223)
Retrying OS detection (try #2) against scrmcfg.sandboxiot.hillrom.com (20.81.62.223)
Initiating Traceroute at 16:15
Completed Traceroute at 16:15, 6.30s elapsed
Initiating Parallel DNS resolution of 15 hosts. at 16:15
Completed Parallel DNS resolution of 15 hosts. at 16:15, 16.53s elapsed
NSE: Script scanning 20.81.62.223.
Initiating NSE at 16:15
Completed NSE at 16:15, 16.31s elapsed
Initiating NSE at 16:15
Completed NSE at 16:15, 4.52s elapsed
Initiating NSE at 16:15
Completed NSE at 16:15, 0.00s elapsed
Nmap scan report for scrmcfg.sandboxiot.hillrom.com (20.81.62.223)

```

4. Webpage Comments and Metadata for Information Leakage:

Description:

Webpage comments and metadata included into the HTML code might reveal internal information that should not be available to potential attackers. Comments and metadata review should be done in order to determine if any information is being leaked.

Expected Output:

We tried to review webpage comments and metadata to better understanding of the application and to find any information leakage.

PoC (Proof of Concept):

```

myts100594@myts100594-Latitude-3400: ~$ curl https://scrmcfg.sandboxiot.hillrom.com/apps/remotemanagement/index.html -v
* Trying 20.81.62.223:443...
* Connected to scrmcfg.sandboxiot.hillrom.com (20.81.62.223) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* CAfile: /etc/ssl/certs/ca-certificates.crt
* CAPath: /etc/ssl/certs
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: CN=*.sandboxiot.hillrom.com
*   start date: Jan 14 13:27:03 2022 GMT
*  expire date: Feb 15 13:27:03 2023 GMT
* subjectAltName: host "scrmcfg.sandboxiot.hillrom.com" matched cert's "*.sandboxiot.hillrom.com"
* issuer: C=US; ST=Arizona; L=Scottsdale; O=GoDaddy.com, Inc.; OU=http://certs.godaddy.com/repository; CN=Go Daddy Secure Certificate Author
*   ty - G2
* SSL certificate verify ok.
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* GET /apps/remotemanagement/index.html HTTP/1.1
* Host: scrmcfg.sandboxiot.hillrom.com
* User-Agent: curl/7.81.0

```

```

myts100594@myts100594-Latitude-3400: ~$ curl https://scrmcfg.sandboxiot.hillrom.com/apps/remotemanagement/index.html -v
* Trying 20.81.62.223:443...
* Connected to scrmcfg.sandboxiot.hillrom.com (20.81.62.223) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* CAfile: /etc/ssl/certs/ca-certificates.crt
* CAPath: /etc/ssl/certs
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: CN=*.sandboxiot.hillrom.com
*   start date: Jan 14 13:27:03 2022 GMT
*  expire date: Feb 15 13:27:03 2023 GMT
* subjectAltName: host "scrmcfg.sandboxiot.hillrom.com" matched cert's "*.sandboxiot.hillrom.com"
* issuer: C=US; ST=Arizona; L=Scottsdale; O=GoDaddy.com, Inc.; OU=http://certs.godaddy.com/repository; CN=Go Daddy Secure Certificate Author
*   ty - G2
* SSL certificate verify ok.
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* GET /apps/remotemanagement/index.html HTTP/1.1
* Host: scrmcfg.sandboxiot.hillrom.com
* User-Agent: curl/7.81.0

```

```

.spinner-snake:before, .spinner-snake:after {
  position: absolute;
  content: '';
  background: #F2F3F2;
}

.spinner-snake:after {
  width: 2.2em;
  height: 4.2em;
  border-radius: 0 2.2em 2.2em 0;
  top: -0.1em;
  left: 2.1em;
  -webkit-transform-origin: 0 2.1em;
  transform-origin: 0 2.1em;
  -webkit-animation: rotator 1s infinite ease;
  animation: rotator 1s infinite ease;
}

@-webkit-keyframes rotator {
  0% { -webkit-transform: rotate(0deg); transform: rotate(0deg); }
  100% { -webkit-transform: rotate(360deg); transform: rotate(360deg); }
}

@keyframes rotator {
  0% { -webkit-transform: rotate(0deg); transform: rotate(0deg); }
  100% { -webkit-transform: rotate(360deg); transform: rotate(360deg); }
}

</style><title>SmartCare Remote Management</title><link rel="preload" href="vendors-branding.b85c59ee933030638367.css" as="style"><lin
k rel="preload" href="vendors-branding.b81858337312495597d1.js" as="script"><link rel="preload" href="branding.d36b311ab12eb2f2e68d.css" as="s
tyle"><link rel="preload" href="branding.afcf152f14a8af624bbd.js" as="script"><link rel="preload" href="vendors-app.b897d5c30a1252b7163.js" a
s="script"><link rel="preload" href="vendors-app.b897d5c30a1252b7163.js" as="script"></head><body><div class="init-load"><div class="spinner-snake"></div><div class="mainlogo"></div>
</body></html>

```


5. Fingerprint Web Application Framework:

Description:

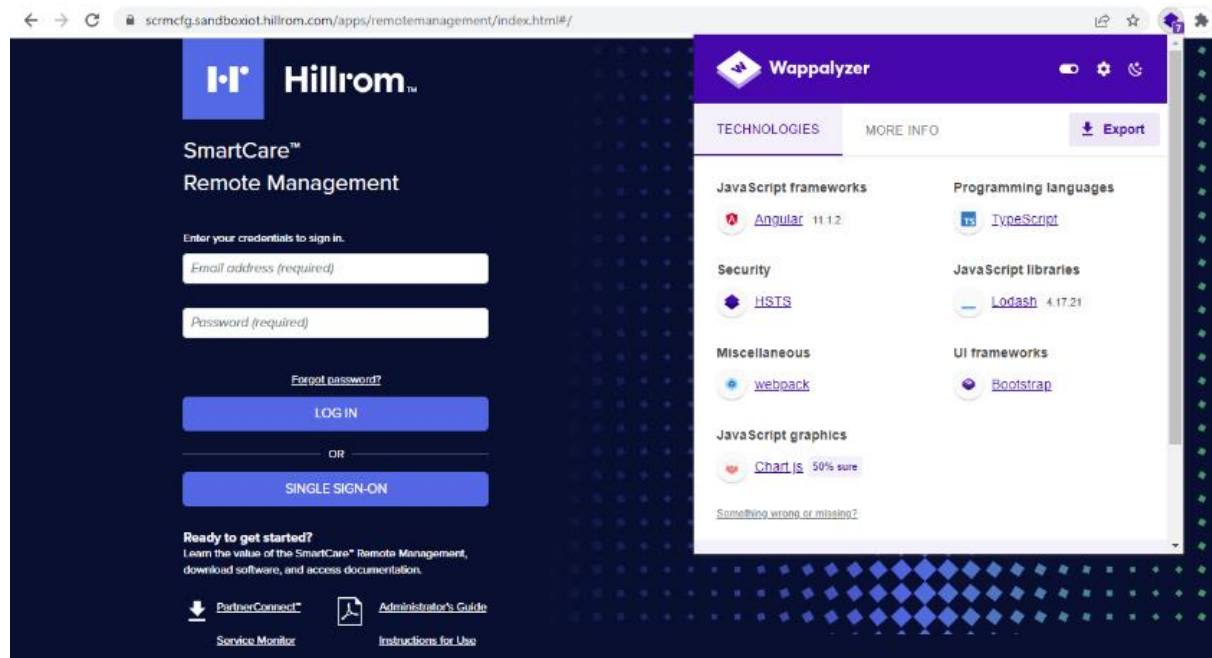
Knowing the web application components that are being tested significantly helps in the testing process and will also drastically reduce the effort required during the test. These well-known web applications have known HTML headers, cookies, and directory structures that can be enumerated to identify the application.

Expected Output:

We tried to fingerprint the components being used by the web applications.

PoC (Proof of Concept):

```
mytsl00594@mytsl00594-Latitude-3400: $ whatweb 20.81.62.223
http://20.81.62.223 [301 Moved Permanently] Country[UNITED STATES][US], IP[20.81.62.223], OpenResty, RedirectLocation[https://20.81.62.223/apps/cockpit/], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[301 Moved Permanently], UncommonHeaders[x-content-type-options]
https://20.81.62.223/apps/cockpit/ [301 Moved Permanently] Country[UNITED STATES][US], IP[20.81.62.223], OpenResty, RedirectLocation[https://20.81.62.223/apps/cockpit/index.html], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[301 Moved Permanently], UncommonHeaders[x-content-type-options]
https://20.81.62.223/apps/cockpit/index.html [200 OK] Bootstrap, Country[UNITED STATES][US], HTML5, IP[20.81.62.223], Script[data], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[Cockpit], UncommonHeaders[x-content-type-options,referrer-policy], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge]
mytsl00594@mytsl00594-Latitude-3400: $
```



6. Map Application Architecture:

Description:

In order to effectively test an application, and to be able to provide meaningful recommendations on how to address any of the issues identified, it is important to understand what you are actually testing. Additionally, it can help determine whether specific components should be considered out of scope for testing.

Expected Output:

We tried to understand the architecture of the application and the technologies in use.

PoC (Proof of Concept):

```
C:\Users\40018075>curl -i https://scrmcfg.sandboxiot.hillrom.com/apps/remotemanagement/index.html#/  
HTTP/1.1 200 OK  
Date: Tue, 13 Dec 2022 11:17:43 GMT  
Content-Type: text/html  
Content-Length: 4054  
Connection: keep-alive  
Last-Modified: Sun, 27 Nov 2022 02:05:36 GMT  
ETag: "6382c5f0-fd6"  
X-Frame-Options: SAMEORIGIN  
X-Content-Type-Options: nosniff  
Referrer-Policy: same-origin  
Expires: Tue, 13 Dec 2022 16:20:29 GMT  
Cache-Control: max-age=18000  
Cache-Control: 5  
Accept-Ranges: bytes  
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

7. Enumerate Infrastructure and Application Admin Interfaces:

Description:

Admin interfaces may be present in the application or on the application server to allow certain users to undertake privileged activities on the site.

Expected Output:

We tried to identify hidden administrator interfaces and functionality.

PoC (Proof of Concept):

```
|---- Scanning URL: https://scrmcfg.sandboxiot.hillrom.com/ ----  
==> DIRECTORY: https://scrmcfg.sandboxiot.hillrom.com/application/  
+ https://scrmcfg.sandboxiot.hillrom.com/apps (CODE:301|SIZE:166)  
==> DIRECTORY: https://scrmcfg.sandboxiot.hillrom.com/identity/  
+ https://scrmcfg.sandboxiot.hillrom.com/index.html (CODE:200|SIZE:1097)  
==> DIRECTORY: https://scrmcfg.sandboxiot.hillrom.com/notification/  
+ https://scrmcfg.sandboxiot.hillrom.com/s (CODE:405|SIZE:546)  
+ https://scrmcfg.sandboxiot.hillrom.com/s1 (CODE:405|SIZE:547)  
+ https://scrmcfg.sandboxiot.hillrom.com/sa (CODE:405|SIZE:547)  
+ https://scrmcfg.sandboxiot.hillrom.com/safe (CODE:405|SIZE:549)  
+ https://scrmcfg.sandboxiot.hillrom.com/safety (CODE:405|SIZE:551)  
+ https://scrmcfg.sandboxiot.hillrom.com/sale (CODE:405|SIZE:549)  
+ https://scrmcfg.sandboxiot.hillrom.com/sales (CODE:405|SIZE:550)  
+ https://scrmcfg.sandboxiot.hillrom.com/salesforce (CODE:405|SIZE:555)  
+ https://scrmcfg.sandboxiot.hillrom.com/sam (CODE:405|SIZE:548)  
+ https://scrmcfg.sandboxiot.hillrom.com/samba (CODE:405|SIZE:550)
```

```

+ https://scrmcfg.sandboxiot.hillrom.com/screenshots (CODE:405|SIZE:556)
+ https://scrmcfg.sandboxiot.hillrom.com/script (CODE:405|SIZE:551)
+ https://scrmcfg.sandboxiot.hillrom.com/scripte (CODE:405|SIZE:552)
+ https://scrmcfg.sandboxiot.hillrom.com/scriptlet (CODE:405|SIZE:554)
+ https://scrmcfg.sandboxiot.hillrom.com/scriptlets (CODE:405|SIZE:555)
+ https://scrmcfg.sandboxiot.hillrom.com/scriptlibrary (CODE:405|SIZE:558)
+ https://scrmcfg.sandboxiot.hillrom.com/scriptresource (CODE:405|SIZE:559)
+ https://scrmcfg.sandboxiot.hillrom.com/scripts (CODE:405|SIZE:552)
+ https://scrmcfg.sandboxiot.hillrom.com/sd (CODE:405|SIZE:547)
+ https://scrmcfg.sandboxiot.hillrom.com/sdk (CODE:405|SIZE:548)
+ https://scrmcfg.sandboxiot.hillrom.com/se (CODE:405|SIZE:547)
+ https://scrmcfg.sandboxiot.hillrom.com/search (CODE:405|SIZE:551)
+ https://scrmcfg.sandboxiot.hillrom.com/search_result (CODE:405|SIZE:558)
+ https://scrmcfg.sandboxiot.hillrom.com/search_results (CODE:405|SIZE:559)
+ https://scrmcfg.sandboxiot.hillrom.com/searchnx (CODE:405|SIZE:553)
+ https://scrmcfg.sandboxiot.hillrom.com/searchresults (CODE:405|SIZE:558)
+ https://scrmcfg.sandboxiot.hillrom.com/search-results (CODE:405|SIZE:559)
+ https://scrmcfg.sandboxiot.hillrom.com/searchurl (CODE:405|SIZE:554)
+ https://scrmcfg.sandboxiot.hillrom.com/sec (CODE:405|SIZE:548)
+ https://scrmcfg.sandboxiot.hillrom.com/seccode (CODE:405|SIZE:552)
+ https://scrmcfg.sandboxiot.hillrom.com/second (CODE:405|SIZE:551)
+ https://scrmcfg.sandboxiot.hillrom.com/secondary (CODE:405|SIZE:554)
+ https://scrmcfg.sandboxiot.hillrom.com/secret (CODE:405|SIZE:551)
+ https://scrmcfg.sandboxiot.hillrom.com/secrets (CODE:405|SIZE:552)
+ https://scrmcfg.sandboxiot.hillrom.com/section (CODE:405|SIZE:552)
+ https://scrmcfg.sandboxiot.hillrom.com/sections (CODE:405|SIZE:553)

```

8. Application Accessible over HTTP:

Description:

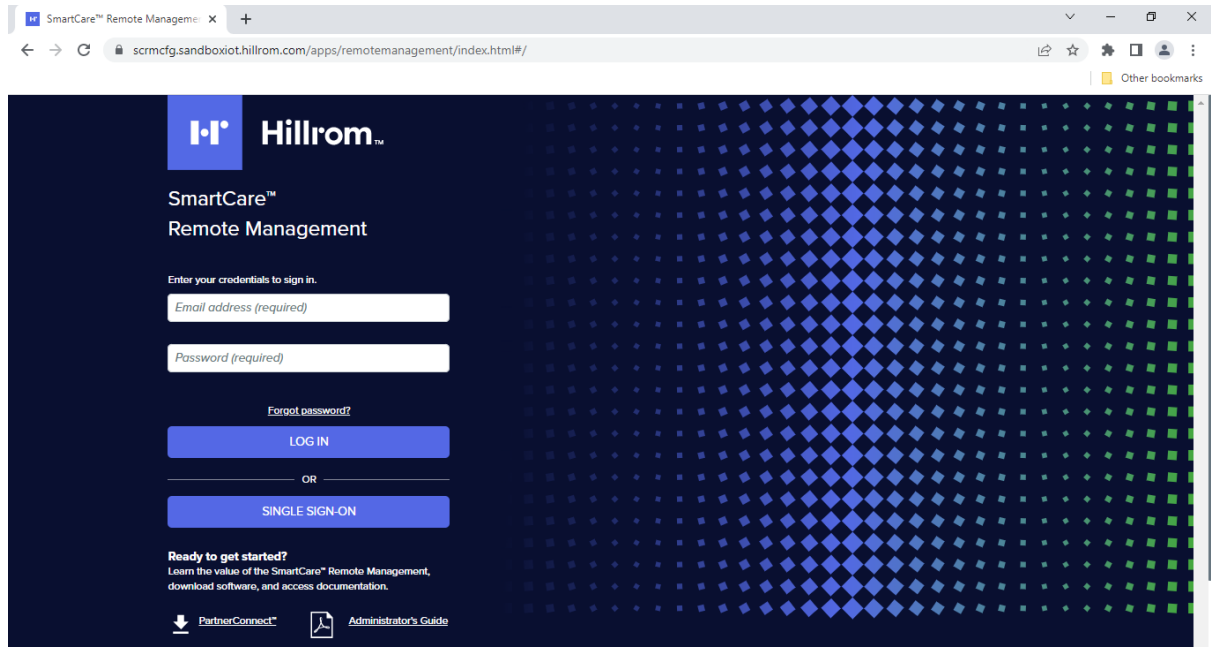
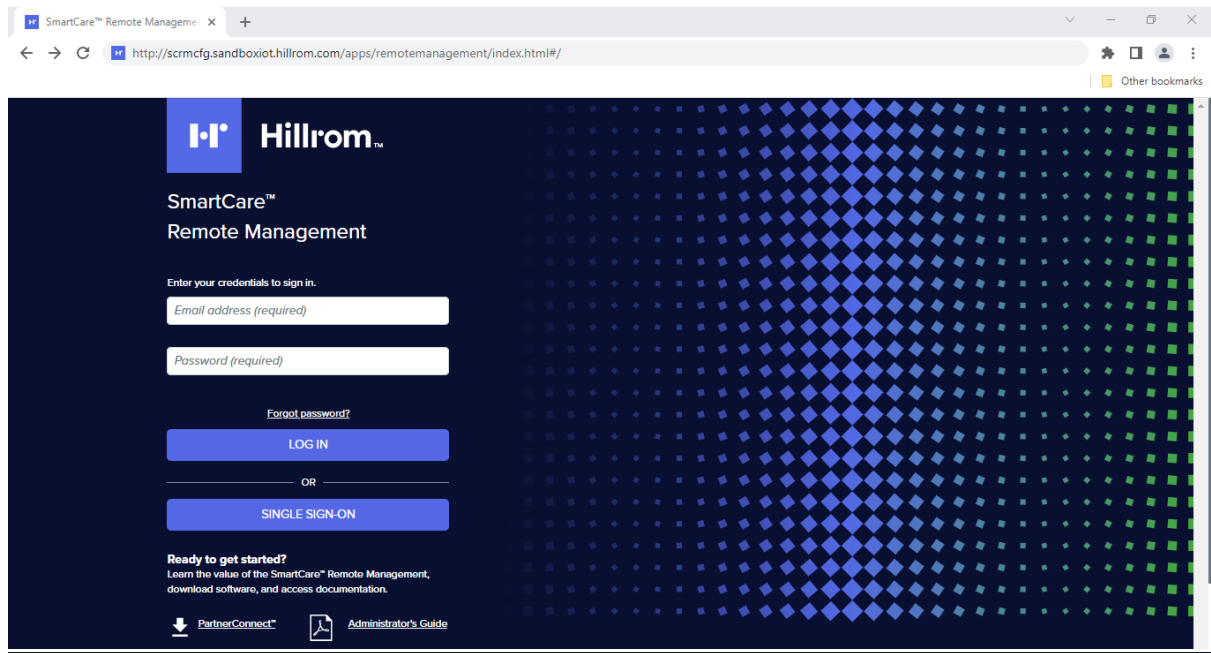
Application doesn't allow web browser to access to the application over HTTP and it redirects to HTTPS. Application redirects to HTTPS and the traffic sent over HTTPS only.

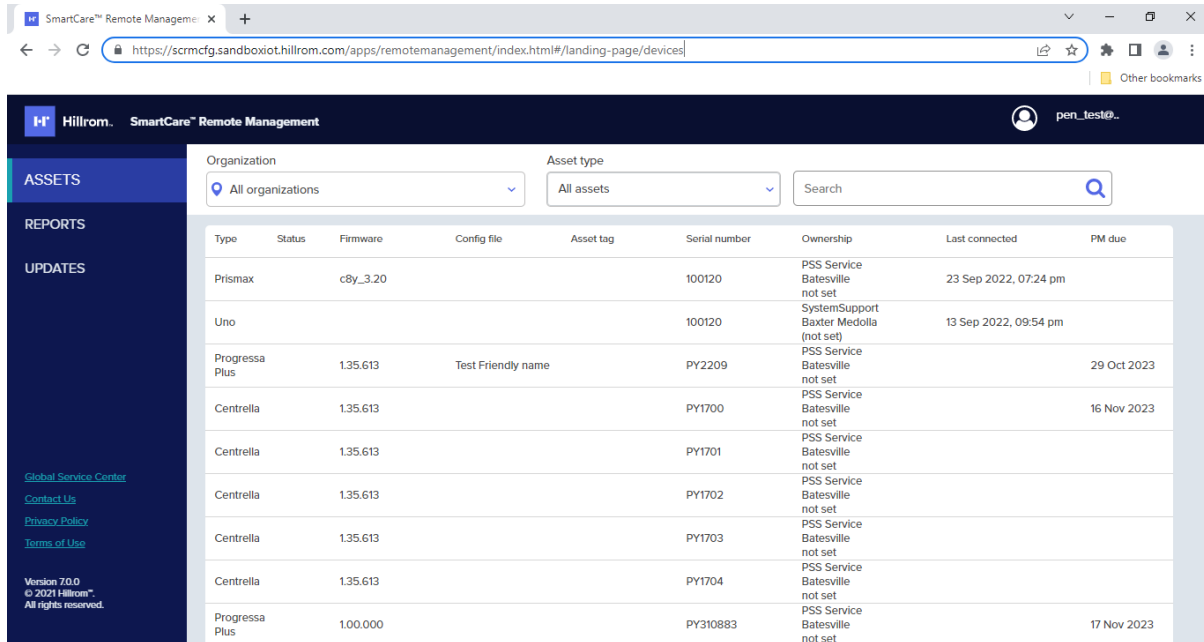
Expected Output:

Application should accessible over HTTP, it should not redirect to HTTPS.

PoC (Proof of Concept):

Security Assessment for SCRM





The screenshot shows the Hillrom SmartCare Remote Management web application. The interface includes a sidebar with navigation links for ASSETS, REPORTS, and UPDATES. The main content area displays a table of assets with columns for Type, Status, Firmware, Config file, Asset tag, Serial number, Ownership, Last connected, and PM due. The table lists several assets, including Prismax, Uno, Progressa Plus, and Centrella, with their respective details.

Type	Status	Firmware	Config file	Asset tag	Serial number	Ownership	Last connected	PM due
Prismax		c8y_3.20			100120	PSS Service Batesville not set	23 Sep 2022, 07:24 pm	
Uno					100120	SystemSupport Baxter Medolla (not set)	13 Sep 2022, 09:54 pm	
Progressa Plus		1.35.613	Test Friendly name		PY2209	PSS Service Batesville not set		29 Oct 2023
Centrella		1.35.613			PY1700	PSS Service Batesville not set		16 Nov 2023
Centrella		1.35.613			PY1701	PSS Service Batesville not set		
Centrella		1.35.613			PY1702	PSS Service Batesville not set		
Centrella		1.35.613			PY1703	PSS Service Batesville not set		
Centrella		1.35.613			PY1704	PSS Service Batesville not set		
Progressa Plus		1.00.000			PY310883	PSS Service Batesville not set		17 Nov 2023

9. Credentials Transported over an Encrypted Channel:

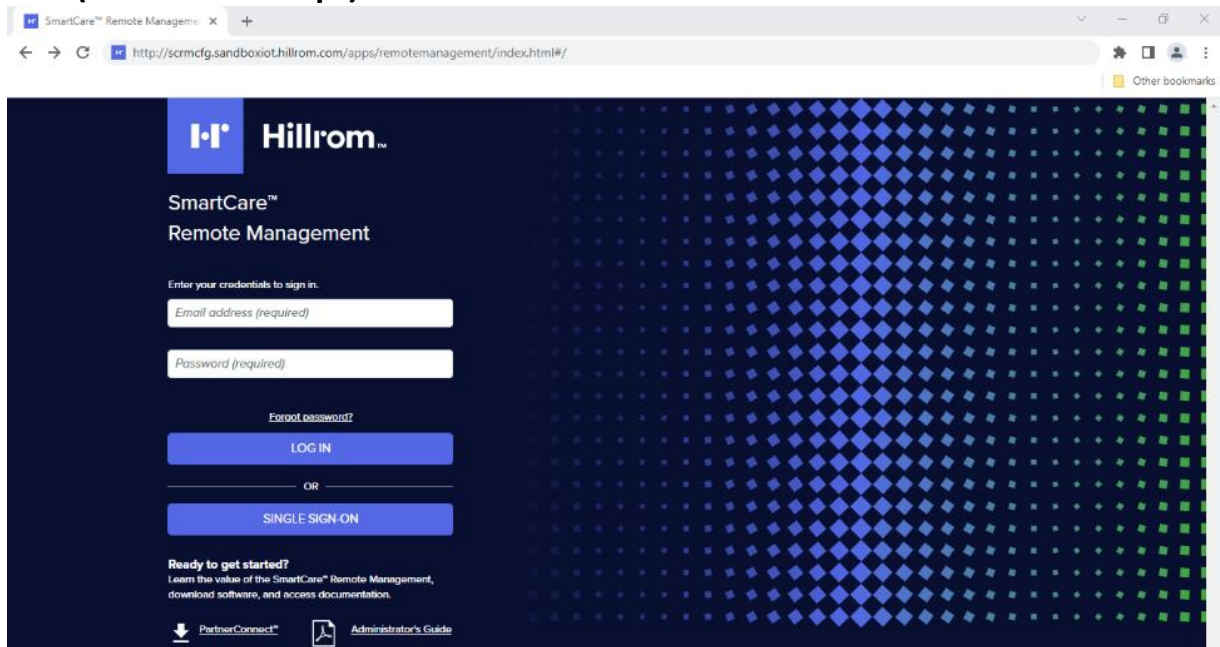
Description:

Verifying that the user's authentication data are transferred via an encrypted channel to avoid being intercepted by malicious users/attackers.

Expected Output:

We expected the credentials which is in weak encryption algorithm or in a plain text.

PoC (Proof of Concept):



Security Assessment for SCRM

The screenshot shows the Hillrom SmartCare Remote Management web interface. The left sidebar contains navigation links: ASSETS, REPORTS, and UPDATES. The main content area displays a table of assets with columns: Type, Status, Firmware, Config file, Asset tag, Serial number, Ownership, Last connected, and PM due. The table lists several assets, including Prismax, Uno, Progressa Plus, and Centrella, with their respective serial numbers and ownership details.

Type	Status	Firmware	Config file	Asset tag	Serial number	Ownership	Last connected	PM due
Prismax		c8y_3.20			100120	PSS Service Batesville not set	23 Sep 2022, 07:24 pm	
Uno					100120	SystemSupport Baxter Medolla (not set)	13 Sep 2022, 09:54 pm	
Progressa Plus		1.35.613	Test Friendly name		PY2209	PSS Service Batesville not set		29 Oct 2023
Centrella		1.35.613			PY1700	PSS Service Batesville not set		16 Nov 2023
Centrella		1.35.613			PY1701	PSS Service Batesville not set		
Centrella		1.35.613			PY1702	PSS Service Batesville not set		
Centrella		1.35.613			PY1703	PSS Service Batesville not set		
Centrella		1.35.613			PY1704	PSS Service Batesville not set		
Progressa Plus		1.00.000			PY310883	PSS Service Batesville not set		17 Nov 2023

10. SQL Injection:

Description:

SQL Injection Scans work through a list of predefined strings that could be used to execute arbitrary SQL code in a database and inserts those strings into the parameters of the request. If an unexpected response is received, this is an indication that input validation has failed to remove the potentially malicious SQL strings from the parameters, and that data should be sanitized before it is used to construct SQL queries.

Expected Output:

We expected to retrieve the user tables, device Id tables, no. of columns and rows, etc.

PoC (Proof of Concept):

```
mytsl00594@mytsl00594-Latitude-3400:~$ sqlmap -u https://scrmcfg.sandboxiot.hillrom.com/apps/remotemanagement/index.html#/landing-page/asset-details?deviceId=81177&deviceType=Prismax
[1] 5219
mytsl00594@mytsl00594-Latitude-3400:~$
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 09:43:41 /2022-12-13/
[09:43:42] [INFO] testing connection to the target URL
[09:43:43] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:43:44] [INFO] testing if the target URL content is stable
[09:43:45] [INFO] target URL content is stable
[09:43:45] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'
[09:43:45] [WARNING] your sqlmap version is outdated
[*] ending @ 09:43:45 /2022-12-13/
mytsl00594@mytsl00594-Latitude-3400:~$ sqlmap -u https://scrmcfg.sandboxiot.hillrom.com/index.php?id=1
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

[illegible]

```
[*] ...  
mySQL00594@mySQL00594-Latitude-3400:~$ sqlmap -u https://scrmcfg.sandboxlot.hillrom.com/apps/remotemanagement/Index.html#/ -data="user=pen_tes  
tuser.com&password=Test@123" -p user -data = POST data  
[3] 5907  
+P: command not found  
mySQL00594@mySQL00594-Latitude-3400:~$  
  
      H  
    [ ] [ ] [ ] [ ] [ ] [ ] {1.6.4#stable}  
   [.] [.] [.] [.] [.] [.]  
  [ ] [ ] [ ] [ ] [ ] [ ]  
 [ ] [V...] [ ] [ ]  
             |_||_|_||_|_  
            https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to ob
ey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by thi
s program

[*] starting @ 09:58:45 / 2022-12-13/

[09:58:45] [INFO] testing connection to the target URL
[09:58:47] [WARNING] the web server responded with an HTTP error code (405) which could interfere with the results of the tests
[09:58:47] [INFO] testing if the target URL content is stable
[09:58:48] [INFO] target URL content is stable
[09:58:48] [INFO] testing if POST parameter 'user' is dynamic
[09:58:50] [WARNING] POST parameter 'user' does not appear to be dynamic
[09:58:51] [WARNING] heuristic (basic) test shows that POST parameter 'user' might not be injectable
[09:58:52] [INFO] testing for SQL injection on POST parameter 'user'
[09:58:52] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:58:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:59:00] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:59:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:59:13] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:59:13] [WARNING] if you experience problems with non-ASCII identifier names you are advised to rerun with '--tamper=charunicodeencode'
[09:59:19] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:59:26] [INFO] testing 'Generic inline queries'
[09:59:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:59:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:59:38] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

11. XML Injection:

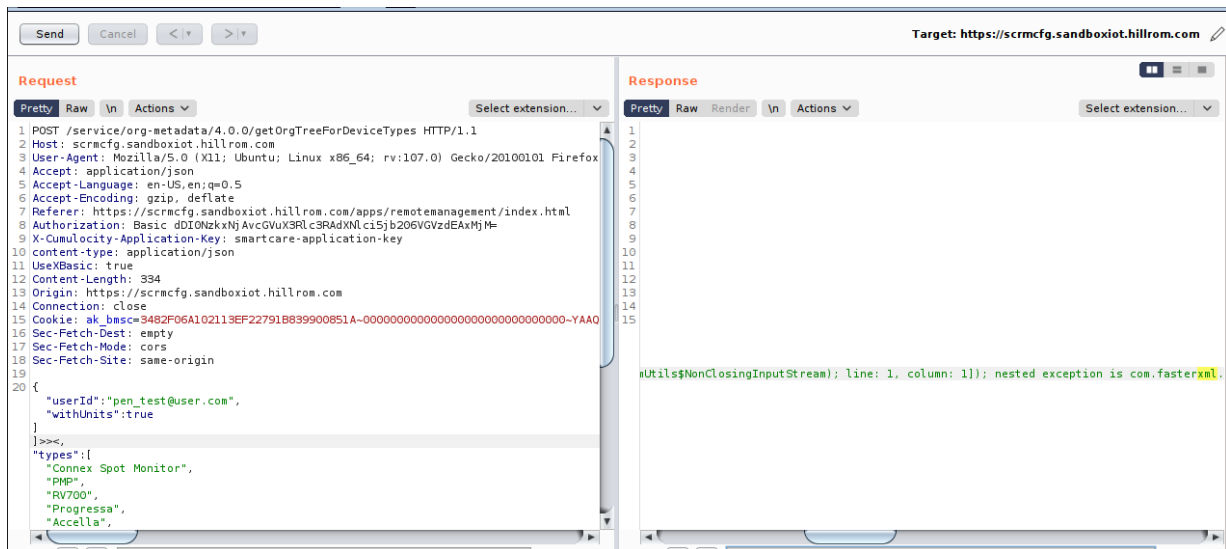
Description:

XML Injection testing is to inject an XML doc to the application. If the XML parser fails to contextually validate data, then the test will yield a positive result.

Expected Output:

We expected to identify XML injection points and assess the types of exploits that can be attained and their severities.

PoC (Proof of Concept):



12. DOM based Cross Site Scripting:

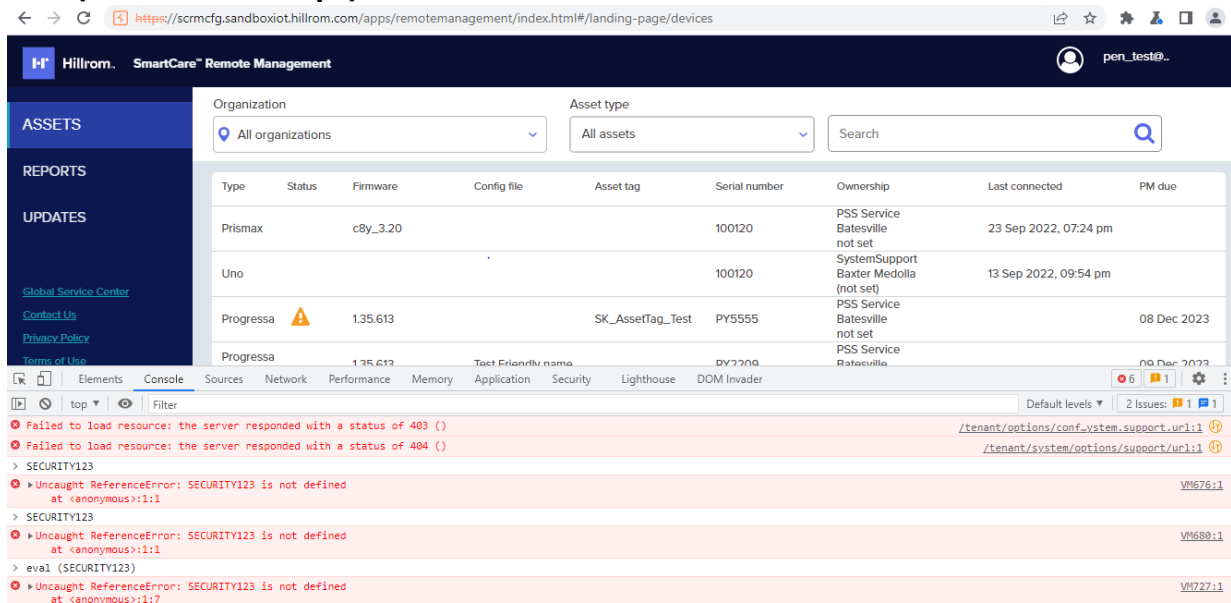
Description:

A DOM based XSS attack is possible if the web application writes data to the Document Object Model without proper sanitization. The attacker can manipulate this data to include XSS content on the web page, for example, malicious java script code.

Expected Output:

We tried used to create a form to let the user choose their preferred language. A default language is also provided in the query string, as the parameter “default”. The page is invoked with a URL such as: A DOM Based XSS attack.

PoC (Proof of Concept):



13. HTML Injection:

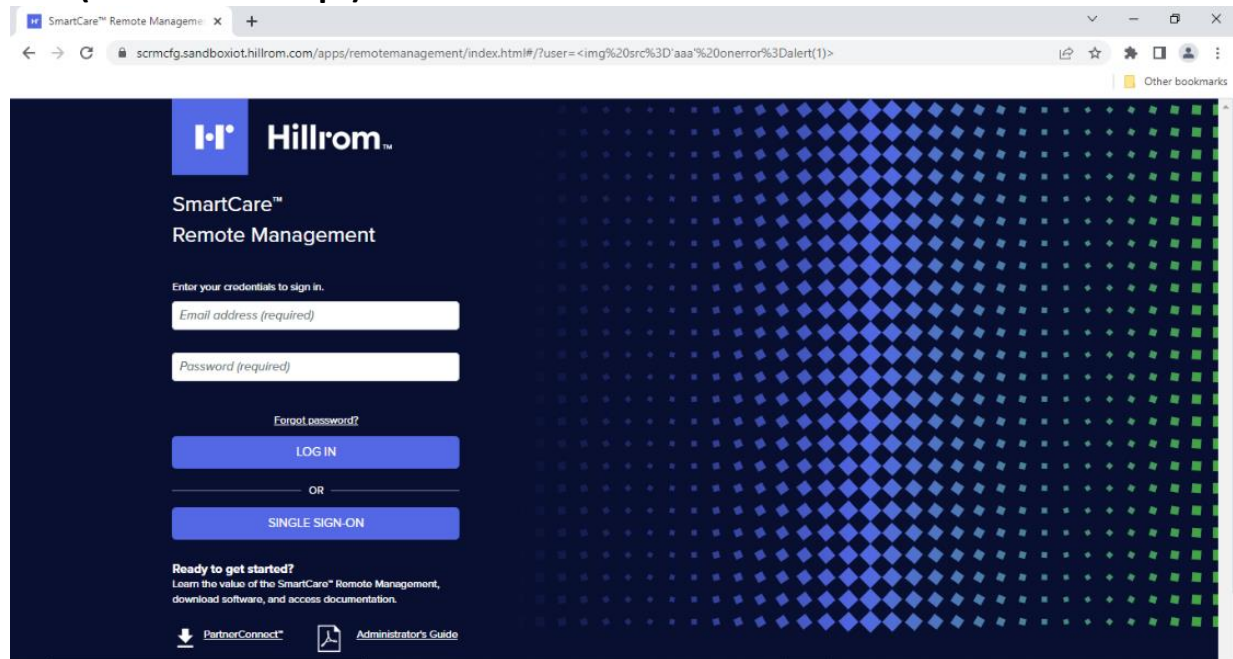
Description:

HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.

Expected Output:

We tried to inject and execute java script code, the HTML injection attack only allows the injection of certain HTML tags. When an application does not properly handle user supplied data, an attacker can supply valid HTML code, typically via a parameter value, and inject their own content into the page. This attack is typically used in conjunction with some form of social engineering, as the attack is exploiting a code-based vulnerability and a user's trust.

PoC (Proof of Concept):



14. XSS Injection:

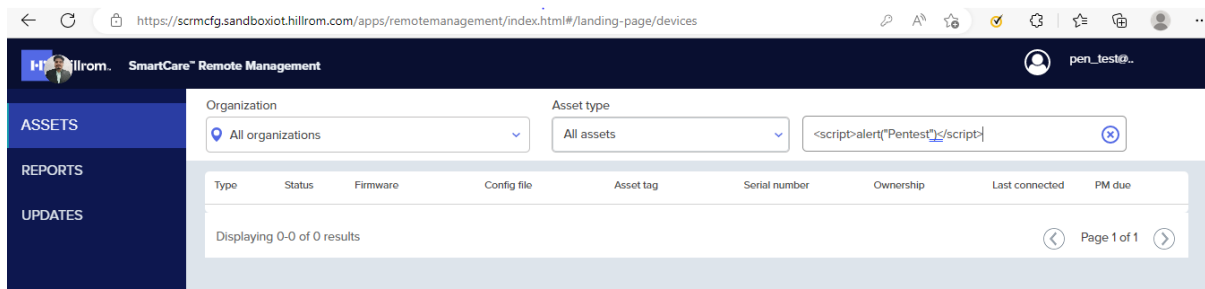
Description:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Expected Output:

We tried to use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

PoC (Proof of Concept):



15. Local Storage:

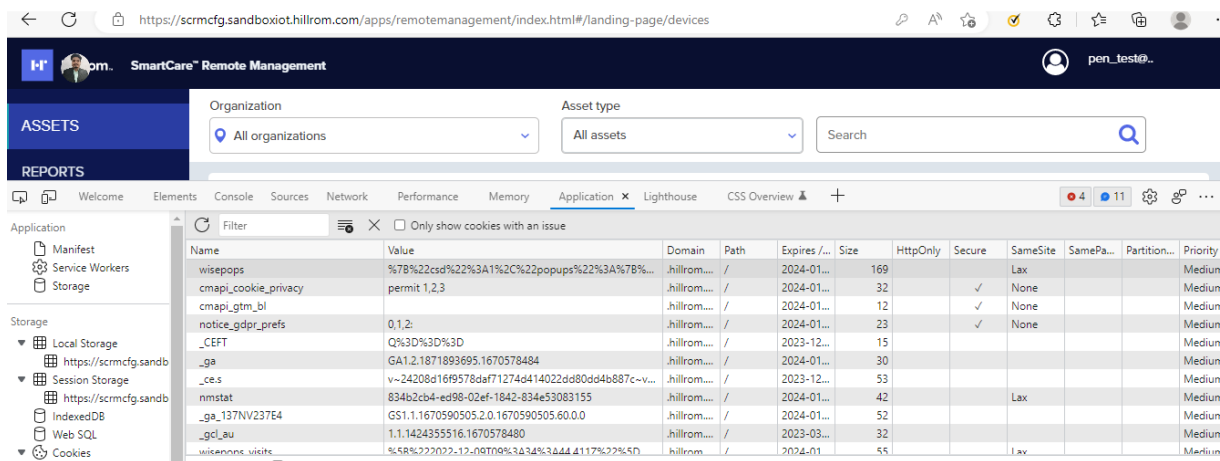
Description:

To store data as key/value pairs tied to a domain and enforced by the same origin policy (SOP). Local Storage that is persistent and is intended to survive browser/system reboots.

Expected Output:

We expected some sensitive data like session id, user credentials, authorization token, JWT (JSON Web Token) token, etc.

PoC (Proof of Concept):



16. Information Exposure of Ports:

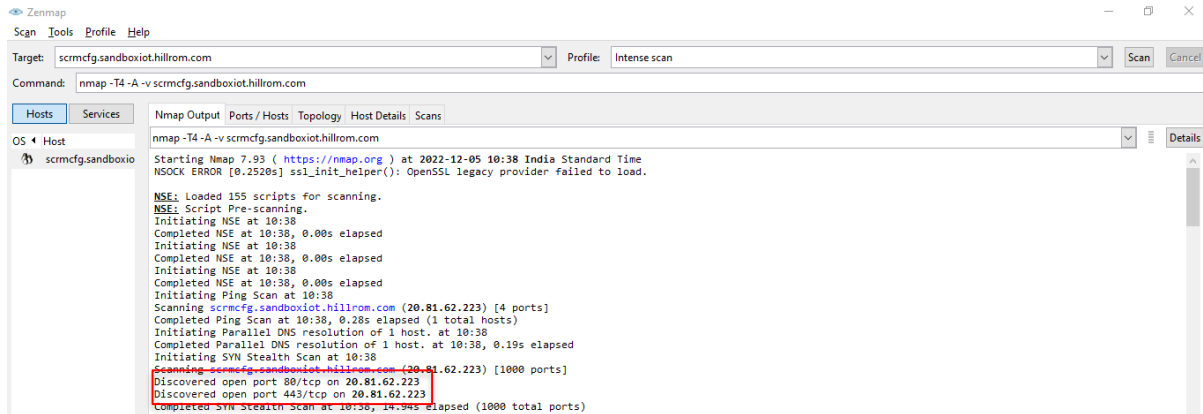
Description:

Security misconfiguration can happen at any level of an application stack, including the network services, web server, application server, database, frameworks, or storage. It is observed that the application displays open ports and servers while performing manual penetration testing. Such flaws frequently give attackers unauthorized access to some system data or functionality.

Expected Output:

We expected to find the ports which are able to use remotely.

PoC (Proof of Concept):



17. Cross Origin Resource Sharing (CORS):

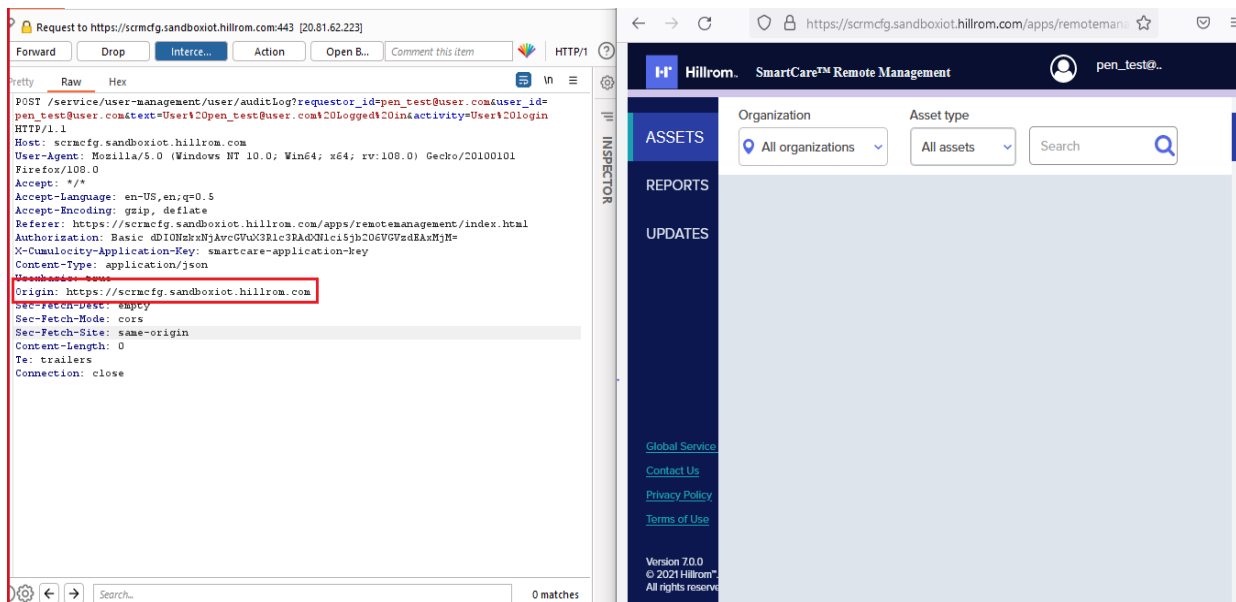
Description:

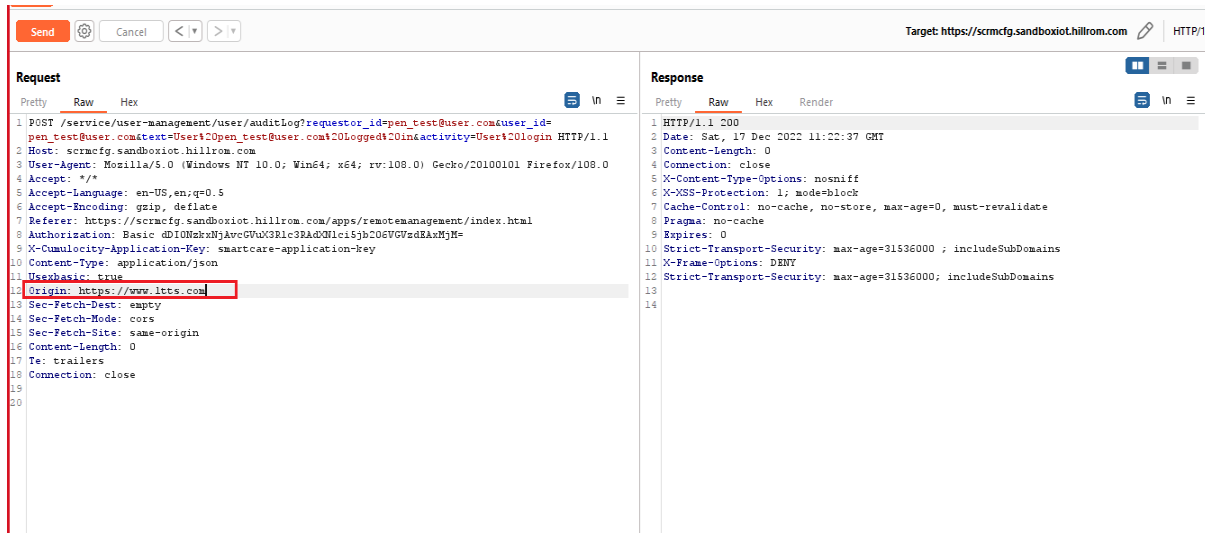
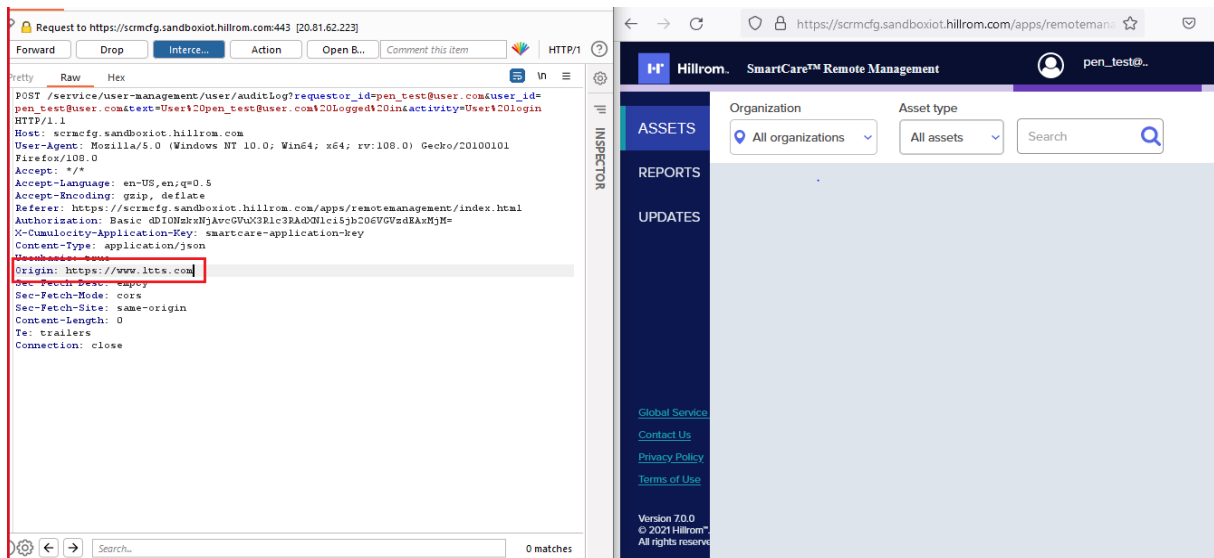
During the assessment, we observed Access-allow control attribute is correctly set using wildcards such as (*) under which domains can request resources. It enables controlled access to resources which are outside of the given domain. It adds flexibility to Same Origin Policy (SOP)

Expected Output:

We tried to find Input Validation Issue: XSS with CORS. Insecure Response with Wildcard * in Access-Control-Allow-Origin.

PoC (Proof of Concept):





18. Clickjacking:

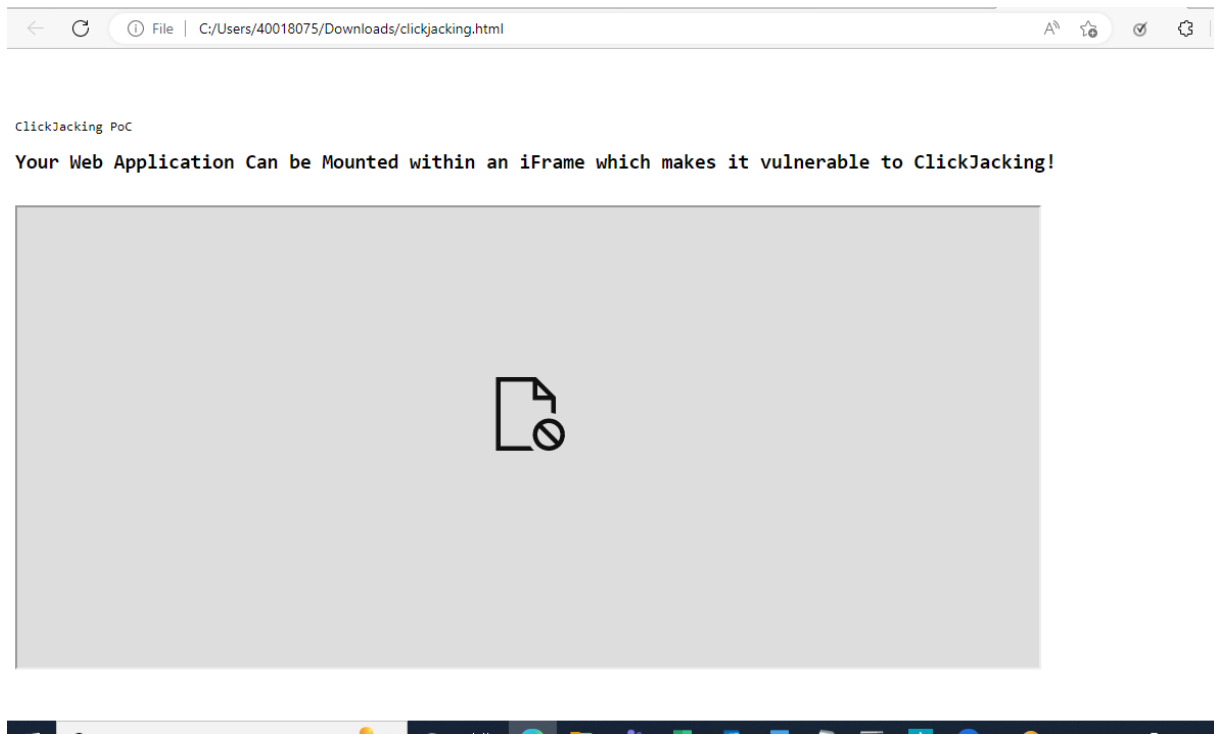
Description:

Clickjacking is a malicious technique that consists of deceiving a web user into interacting by clicking with something different to what the user believes they are interacting with. This type of attack, that can be used alone or in combination with other attacks, could potentially send unauthorized commands or reveal confidential information while the victim is interacting with seemingly harmless web pages. User Management has many instances where pages are missing X-frame headers to avoid clickjacking.

Expected Output:

We tried to perform by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

PoC (Proof of Concept):



19. WebSockets:

Description:

WebSockets are widely used in modern web applications. They are initiated over HTTP and provide long-lived connections with asynchronous communication in both directions. WebSockets are used for all kinds of purposes, including performing user actions, and transmitting sensitive information. Virtually any web security vulnerability that arises with regular HTTP can also arise in relation to WebSockets communications.

Expected Output:

We tried to manipulate WebSocket messages, it is sometimes necessary to manipulate the WebSocket handshake that establishes the connection.

PoC (Proof of Concept):

Security Assessment for SCRM

WebSockets message to https://scrmcf.sandboxiot.hillrom.com/notification/realtime

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 [{
  "ext": {
    "com.cumulocity.authn": {
      "token": "dDIONzKxNjAvcGVuZC3Rlc3RAZDQ1Ici5jb206VGUzdEAxMjM="
    }
  },
  "id": "5",
  "version": "1.0",
  "minimumVersion": "1.0",
  "channel": "/meta/handshake",
  "supportedConnectionTypes": [
    "websocket",
    "long-polling",
    "callback-polling"
  ],
  "advice": {
    "timeout": 60000,
    "interval": 0
  }
}]
```

Send Cancel < >

Target: https://scrmcf.sandboxiot.hillrom.com HTTP/1

Request

Pretty Raw Hex

```
1 GET /notification/realtime HTTP/1.1
2 Host: scrmcf.sandboxiot.hillrom.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Sec-WebSocket-Version: 13
8 Origin: https://scrmcf.sandboxiot.hillrom.com
9 Sec-WebSocket-Key: WW0Qrp7QoYU+D60yS8Uz4q==
10 Connection: keep-alive,, Upgrade
11 Sec-Fetch-Dest: websocket
12 Sec-Fetch-Mode: websocket
13 Sec-Fetch-Site: same-origin
14 Pragma: no-cache
15 Cache-Control: no-cache
16 Upgrade: websocket
17
18
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 101 Switching Protocols
2 Date: Fri, 16 Dec 2022 09:02:18 GMT
3 Connection: upgrade
4 Sec-WebSocket-Accept: t76Ky9UeKOK3j4F3UUHIS9a2+mg=
5 Upgrade: WebSocket
6 X-Content-Type-Options: nosniff
7 Strict-Transport-Security: max-age=31536000; includeSubDomains
8
9
```

3. Abbreviation

APP	Application
HTML	Hypertext Mark-up Language
HTTP(S)	Hypertext transfer protocol (Secured)
Pg.	Page
TLS	Transport Layer Security
SSL	Secure Sockets Layer
IP	Internet Protocol
LTTS	Larsen & Toubro Technology Services
SOP	Same Origin Policy
OWASP	Open Web Application Security Project
VAPT	Vulnerability Assessment and Penetration testing
CORS	Cross Origin Resource Sharing
XSS	Cross-Site Scripting
HTML	Hypertext Markup Language
DOM	Document Object Model
SQL	Structured Query Language